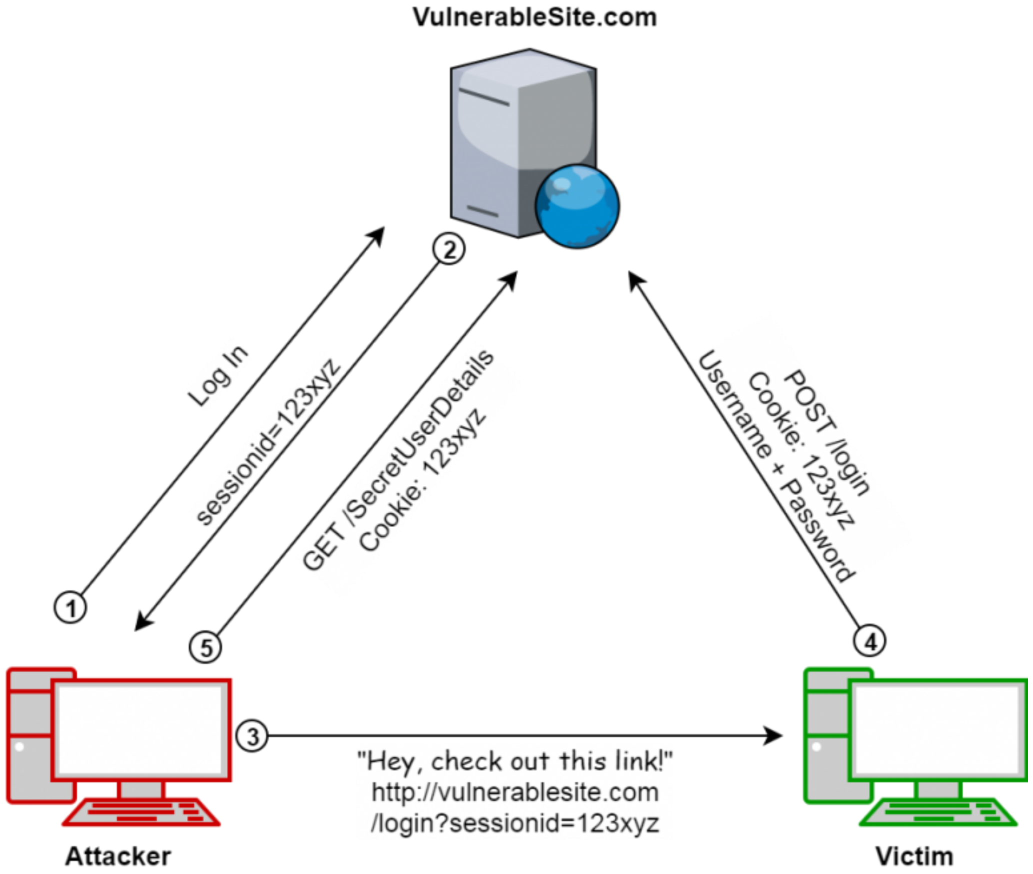
Session Fixation

What is a Session?
The activity done by the user from the second he logs into a web application until he logs out of it is called a session.
A session can temporarily store information related to the activities of the user while connected. A session cookie is used in web pages for storing information in case the user leaves the web page or closes their Internet browser.

What is Session Fixation?
Session Fixation is an attack that permits an attacker to hijack user sessions. It fixes the user's session in a different device by using the session id as the only authentication. The attacker attempts to steal the ID of a victim's session after the user logs in.
If the web application is vulnerable, the victim's session is created in the attacker's device without credentials.



A typical session fixation attack is performed as follows:

1. The attacker accesses the web application login page and receives a session identifier generated by the web application.
2. The attacker uses an additional technique such as CRLF Injection, man-in-the-middle attack, social engineering, etc., and gets the victim to use the provided session identifier.
3. The victim accesses the web application login page and logs in to the application. After authenticating, the web application treats anyone who uses this session ID as if they were this user.
4. The attacker uses the session identifier to access the web application, take over the user session, and impersonate the victim.

Steps to Reproduce:
1. Login into account
2. Export cookies using cookie editor extension/burp
3. Open the same website in another browser
4. Delete old cookie from cookie editor
5. Import old cookies
6. Refresh > If we are logged in, the website is vulnerable.

Session Hijacking

What is Session Hijacking?
Session hijacking is as the term suggests. A user in a session can be hijacked by an attacker and lose control of the session altogether, where their personal data can easily be stolen. After a user starts a session, such as logging into a banking website, an attacker can hijack it.

In order to hijack a session, the attacker needs to have substantial knowledge of the user's cookie session. Although any session can be hacked, it is more common in browser sessions on web applications.

What is the difference between Session Fixation and Session Hijacking?

Session fixation and session hijacking are both attacks that attempt to gain access to a user’s client and web server session. In the session hijacking attack, the attacker attempts to steal the ID of a victim's session after the user logs in. In the session fixation attack, the attacker already has access to a valid session and tries to force the victim to use that particular session for his or her own purposes. The session fixation attack “fixes” an established session on the victim's browser, so the attack starts before the user logs in.

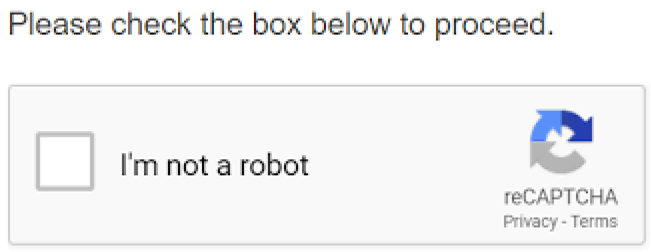
Session fixation attacks are designed to exploit authentication and session management flaws. Any system that allows one person to fixate another person's session identifier is vulnerable to this type of attack. Most session fixation attacks are web-based, and most rely on session identifiers being accepted from URLs or POST data.

Captcha Bypass

What is Captcha Bypass?

A CAPTCHA is a type of challenge-response test used in computing to determine whether the user is human. Bypassing this is called captcha bypass.

Typically, an attacker can create a bot to bypass the captcha and automate the tasks to send unlimited requests to multiple URLs or lists with random/fake users, emails, IP address. for spamming or evil purposes.



Please check the box below to proceed.

Methods to bypass captcha

1. **Change the request method:**
   It is an easy method to check for bypassing captcha just by changing the "request method of your request" and removing the captcha parameter
2. **Remove the captcha parameter/reuse the old captcha**
3. **Use extra headers**
   X-Originating-IP: 127.0.0.1
   X-Forwarded-For: 127.0.0.1
   X-Remote-IP: 127.0.0.1
   X-Remote-Addr: 127.0.0.1
4. **Use https://book.hacktricks.xyz/pentesting-web/captcha-bypass**

References

https://www.acunetix.com/blog/web-security-zone/what-is-session-fixation/

https://secureteam.co.uk/articles/web-application-security-articles/understanding-session-fixation-attacks/

https://www.appsecmonkey.com/blog/session-fixation

https://us.norton.com/internetsecurity-id-theft-session-hijacking.html

https://www.globalsign.com/en/blog/session-hijacking-and-how-to-prevent-it

https://www.venafi.com/blog/what-session-hijacking

https://www.contrastsecurity.com/glossary/session-fixation-attack#:~:text=In%20the%20session%20hijacking%20attack,his%20or%20her%20own%20purposes.

https://medium.com/@honeyakshat999/captcha-bypass-techniques-f768521516b2